SECURE AND ENERGY AWARE DATA TRANSMISSION FOR IOT BASED WIRELESS SENSOR NETWORKS USING BLOCKCHAIN TECHNOLOGY

A SYNOPSIS

Submitted by

P. VELMURUGADASS
(Reg. No. 201907267)

in partial fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SCHOOL OF COMPUTING
KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
ANAND NAGAR, KRISHNANKOIL - 626 126

NOVEMBER - 2022

1. INTRODUCTION

In today's world, everything around us is connected to the Internet of things (IoT) environment. Cloud computing technology offers unlimited storage with other valuable on-demand computing resources for IoT users. Wireless Sensor Networks (WSNs) have recently experienced rapid growth in the IoT era [1]. WSNs are becoming an emerging technology for potential applications, such as surveillance systems, agriculture, environmental monitoring, domestic, disaster management, and health care [2]. WSNs comprise various nodes (sensors) that can be placed anywhere in the world to sense, compute, monitor, and communicate with other networks [3]. One (or more) centralized control units called base stations have been used in WSNs. A base station (BS) is often used as a gateway to another network, providing excellent storage and data processing capabilities and a human interface access point [4]. Sensors in WSNs are typically low-cost and require less battery power, making them energy-constrained. The main issue in WSNs is increasing network lifetime when the initial node cannot transmit the data toward the sink node.

The clustering strategy is a scheme that aims to improve WSN's energy efficiency (EE) and the network's lifetime by balancing EC. This strategy categorizes nodes into independent clusters with geographically close nodes and divides the network topology logically into a hierarchical structure. Cluster Heads (CHs) collect information from the nodes within a corresponding cluster and compress it before sharing it with the BS or sink. The optimal cluster head (CH) selection framework reduces energy, delay, distance, and so on. The researchers develop many methodologies to achieve a better CHs selection process in WSNs. However, the algorithm frequently suffers from several flaws, including a poor exploitation phase, a slow convergence rate, and a limited ability to solve multi-objective problems. Furthermore most of these CH selection algorithms are only concerned with the EE of the network. In addition, they did not consider the security of CH nodes. As a result, there is a need for an algorithm to securely select CHs by perceiving the bargained hubs and denying them CH candidacy in WSNs [5, 6].

When users want to communicate securely with SNs, they must perform mutual authentication and key agreement. Therefore secure and mutual authentication, in addition to secret key agreement protocol, is a powerful cryptographic tool for WSNs. Most security solutions rely heavily on the centralized system and third-party service providers. However, this mechanism has a single point of failure (SPOF), many-to-one traffic, and limited

scalability [7]. Most of the time, they cannot deal with a strong attacker due to its resource-restricted nature. As a result, securing sensing data and sensing readings in WSNs is critical. Blockchain (BC) is a newly developed decentralized infrastructure and a distributed computing model that has been thoroughly researched and used in recent years [8]. Integrating BC capabilities into the WSNs will enable the creation of next-generation networks, whose nodes will be fully protected and able to conduct transactions autonomously through smart contracts without the need for a single point of failure, making them completely decentralized [9]. According to the analysis, the significant challenges of the IoT-assisted WSN include EE, quality of service (QoS), and security. Researchers conducted many studies on IoT-based WSNs for enhancing EE, QoS, and security. However, every work focuses on a specific goal. As a result, to achieve better performance, a novel IoT-WSNs design is required.

2. LITERATURE SYRVEY

Bharat Bhushan and Gadadhar Sahoo [10] presented a Fuzzy Logic-based Energy Adequate Clustering (FLEAC) method for selecting suitable CHs for DA in WSNs. The protocol contemplated using relay nodes (RNs) to reduce the excessive energy consumption (EC) of CHs. The data was collected by the CHs and sent to the RNs, who relayed it to the BS. The protocol outperformed comparable protocols regarding EC and network lifetime. **Amol V. Dhumane and Rajesh S. Prasad** [11] created a multi-objective fractional gravitational search algorithm (MOFGSA) for determining the best CH for an energy-efficient routing protocol in an IoT network. The fitness function selected the CHs based on multiple objectives like delay, distance, energy, and link lifetime. The findings demonstrated the MOFGSA's superiority over existing techniques. **Kavita Jaiswal and Veena Anand** [12] presented a CH selection technique for WSNs based on Grey wolf optimization (GWFO). The author also discussed routing via QoS-aware relay node selection for an efficient and dependable inter-cluster routing from CHs to BS. The techniques improved the network's overall performance when compared to existing schemes. **Mohana Bakshi et al.** [13] proposed a glow-worm swarm optimization-based adaptive CH selection algorithm (GWSO). The algorithm partitioned the entire network into an optimal number of clusters. The algorithm performed significantly better than the state-of-the-art IoT clustering protocol, even when more than 20% of the nodes ran out of energy. **Vasim Babu et al.** [14] presented a secure routing (SR) approach with the help of implementing the following models. Firstly the author established a Distributed Autonomous Fashion with Fuzzy If-then Rules (IDAF-FIT)

to cluster the SNs in WSN. The author introduced an Adaptive Source Location Privacy Preservation (ASLPP) method utilizing Randomized Routes (RR). Further, Secure DA using Principle Component Analysis (SDA-PCA) was introduced with privacy and strength. The results indicated that the model increased the accuracy and decreased the estimation errors, EC and overhead**.**

Akash Suresh Patil *et al*. [15] have presented a successful privacy-preserving authentication protocol using BC and a secret computational model based on Physically Unclonable Functions (PUF). Every device in the network had to first register with the smart contract using its device ID and PUF approach. The smart contract performed verification and validation when an IoT transmitted data. It terminates the request of the device if it is not listed in a trusted device list. Otherwise, it stored the data in a BC. **Azath Mubarakali** [16] presented a BC-centered micro-WSN identity authentication framework for decentralized data delivery. The study first established a BC-enabled sensor network betwixt cluster managers in a WSN and included every WSN ground station in the public BC. Then the study installed a hybrid BC framework across the whole network. Betwixt network and ordinary nodes, the identity data registration was carried out, and the connectivity authorization betwixt clusters was carried out. **Qing Fan et al.** [17] presented a BC-based effectual authentication and data-sharing scheme for IoT. The model utilized an enhanced ID-based signature authentication and secures data transmission (DT) scheme for IoT, ensuring authenticity, integrity, and information privacy. The author developed this model to accomplish mutual authentication betwixt the perception layer and network layer and provide secure DT betwixt the application layer and the network layer.

Semih Cakir et al. [18] utilized a Gated Recurrent Unit (GRU) network to identify and prevent Hello Flooding (HF) attacks performed on the Routing Protocol for Low-Power and Lossy Networks (RPL) in IoT. The architecture was divided into three sections: network simulation, preprocessing of data, and attack detection. The results confirmed that the expected source efficiency and IoT security performance were better than the existing methods. **Premkumar and Sundararajan** [19] adapted deep learning-based Radial basis networks (DRBN) for attack detection and isolation in WSNs. The key management system's key launch, route launch, and data forwarding phases were all described. The DRBN system produced the most effective results and outperformed several state-of-the-art techniques. **Gethzi Ahila Poornima and Paramasivan** [20] suggested an Online Locally Weighted Projection Regression (OLWPR) for detecting anomalies in WSNs. Principal

Component Analysis (PCA) was used to lessen the dimensionality of OLWPR. Compared to other models, the outcomes showed that the presented technique achieved a higher detection rate and a lesser false alarm rate.

3. PROBLEM STATEMENT

Unequal clustering, higher EC, algorithm's complexity, lack of population diversity, getting stuck in local minima in the last iterations, and an imbalance between exploitation and exploration are all drawbacks of the models developed for energy-efficient CH selection. They only focused on developing models for diminishing the EC and enhancing network lifetime. They should have prioritized network security, resulting in unauthorized data access and intruder attacks on sensed data. The BC-based authentication models failed to address the better security issue and achieved a higher data integrity rate and a shorter processing time. Furthermore, they could not implement a robust cryptographic mechanism to ensure the security of transmitted data. Furthermore, none of these approaches has developed an integrated solution for detecting attacks on data in WSNs. Existing attack detection systems were prone to false detection due to classifiers' poor convergence rate and the imprecise selection of features required for attack classification. Overall, QoS and security provisioning with EE suffers due to increased time complexity, EC, and poor algorithm design. As a result, we are motivated to address the research challenges of improving security and QoS without compromising EE in this work.

4. RESEARCH OBJECTIVES

- To propose efficient authentication scheme for preventing unauthorized user access in the network.
- To propose an efficient clustering technique and optimal CH selection algorithm to improve the EE, network lifetime, and QoS parameters.
- To propose robust encryption schemes for providing data security in the IoT network.
- To propose a deep learning model with an optimal feature selection approach to perform security analysis of the network.
- To provide secure cloud storage for authentication credentials and IoT data.

5. RESEARCH METHODOLOGY

5.1 Enhancing Blockchain Security in Cloud Computing with IoT Environment using ECIES and Cryptography Hash Algorithm

This research developed a novel mechanism to perform authentication and encryption in IoT using software-defined networks (SDN) and BC. Initially, the user is registered to the trusted authority and receives the key for data encryption using HSO. The user is then authenticated by a trusted authority using a user id, password and a random number. After successful authentication, the user encrypts their data and uploads it to the cloud. An elliptic curve integrated encryption scheme (ECIES) is used for encryption. The user data is encrypted using ECIES twice for sensitive data and only once for non-sensitive data. Then, the encrypted data is stored in the cloud through the switches. The SDN controller uses a BC mechanism to store the user's encrypted data. In a BC, a block for each data the user uploads is created. The block contains a list of transactions, the hash value (SHA-256) of data, the previous block, and a time stamp value. Any modification performed on these data can be traced using the smart contract. In the end, the user can get the evidence of data modification that is performed on their uploaded file with the help of a trusted authority investigator as a logical graph of evidence (LGoE). The architecture of the proposed research framework is given in Figure 1.

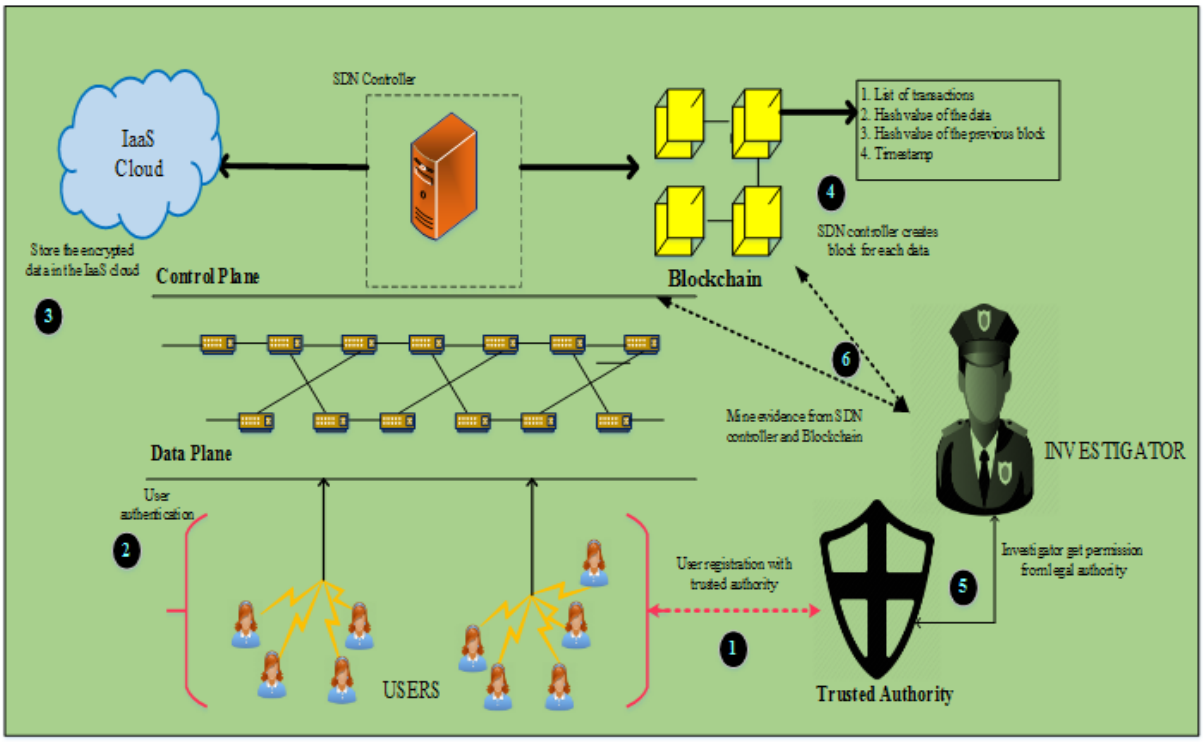


Figure 1: Architecture of the proposed SDN based BC and ECIES cryptographic model

5.1.1 Performance Evaluation

The results of the proposed system are evaluated by plotting the encryption time and decryption time of the ECIES for encrypting the users' different uploaded file sizes. The existing models taken for comparison are Rivest-Shamir-Adleman (RSA) and Blowfish Algorithm (BFA). Figure 2 shows that the proposed model achieves better performance regarding encryption and decryption time for varying file sizes (100MB, 200MB, 300MB, 400MB, and 500MB). This lowest value of these metrics shows the efficiency of the proposed model for data security in IoT over others.

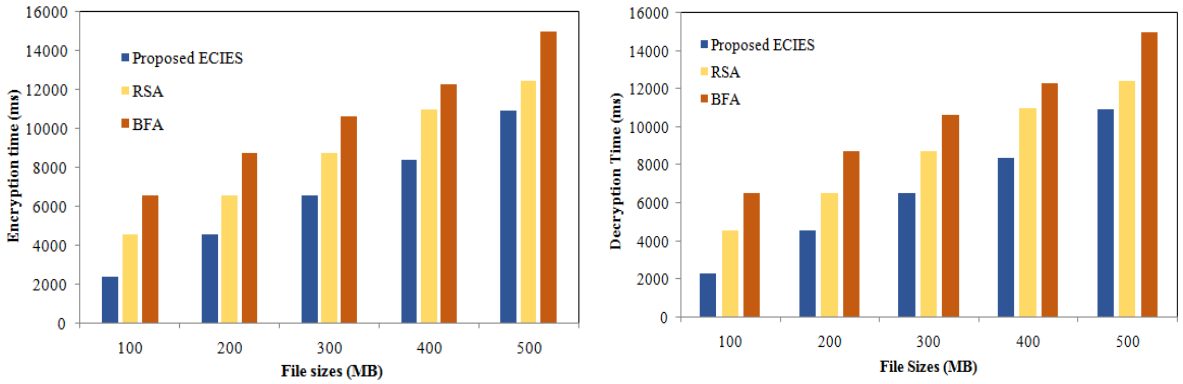


Figure 2: Performance efficiency of the proposed ECIES over existing RSA and BFA

5.2 QoS Aware Secure Data Transmission Model for IoT Assisted Wireless Sensor Networks

In IoT-assisted WSNs, many tiny sensor devices are used in every application to send the sensed report to the BS. When operating in a distributed WSN, user terminals and other network entities can attain original data directly from SNs. However, these sensor devices are resource constrained because of the limited battery power, and they have less access to heterogeneous resources because of the deployment region and communication technology. In addition, the nodes use open wireless channels for the process of communication as well as to access information. These two features offer a threat of vulnerability across the network. Thus, to address these issues, a BC-based secure data storage system is proposed in this work using SN authentication and encryption techniques. The proposed work comprises the following phases: WSN sensor node initialization, registration, clustering, CHs selection, authentication, data encryption, and finally, the BC stores the data in the cloud. Figure 3 portrays the architecture of the proposed research framework.

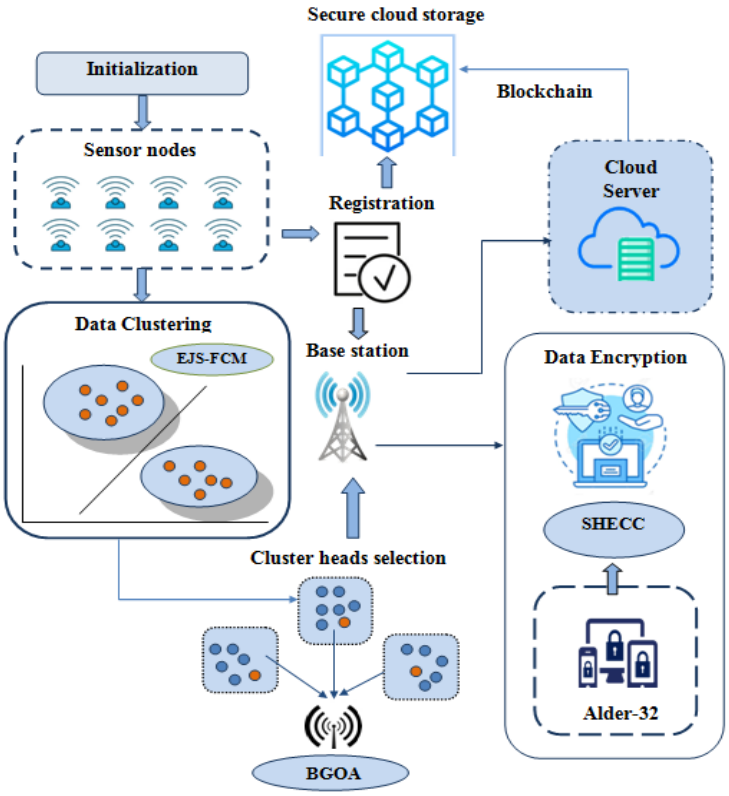


Figure 3: Architecture of the proposed QoS aware secure DT model

5.2.1 Sensor Node Initialization and Registration

Firstly the sensor nodes (SNs) are deployed in the environment with the help of BS. Next, the SNs send a registration request to the BS. For each request of SNs, the BS creates the identification number (ID^i) and forwards it to the SNs. Then, the BS creates the secret key (λ) for node authentication purposes using the three parameters such as node's identification number, time of node's registration, and a secret number selected randomly in the range [0, 1]. Next, the secret key is converted into hash code using the Adler-32 hashing technique. The Adler-32 hashing technique generates quick hashes, has a tiny space, and is more secure than other cryptographic hashing. After generating the hash code, the BS sends it to the CH, which will further be used in the authentication process. The authentication credentials obtained from the IoT devices are stored in a BC for security purposes.

5.2.2 Clustering with EJS-FCM

For energy-efficient DT and to maximize network lifetime, the SNs are grouped using the Entropy-based Jaccard Similarity-induced Fuzzy C-Means (EJS-FCM) algorithm. FCM is used in this case because it is efficient, simple, and has a quick convergence time. The general FCM's Euclidean distance (ED) calculation is more complicated, which degrades the

clustering results. As a result, the ED is replaced in the proposed work by the Jaccard Similarity (JS) measure, which is easy to calculate and clusters data more precisely. The data's entropy value is also used to select the initial centroids. The algorithmic steps of EJS-FCM are given as follows and the process continues until the objective function is smaller and maps the data to the smallest cluster center.

Step 1: Let the input to the EJS-FCM be the N number of SNs $S^i = S^1, S^2, \ldots\ldots S^N$, which are partitioned into K number of clusters.

Step 2: Then, the initial cluster centroids are calculated based on the entropy value. The entropy $\langle E(S^i) \rangle$ is calculated using the below equation,

$$E(S^i) = \sum_{i=1}^{N} p(S^i) \cdot \log p(S^i)$$

Based on the above calculation, the EJS-FCM generates M number of initial centroids (C^j), which are denoted as

$$C^j = C^1, C^2, \ldots\ldots, C^M$$

Step 3: The EJS-FCM attempts to minimize the objective function (η) which is given by,

$$\eta = \sum_{i=1}^{N} \sum_{j=1}^{M} \mu_{ij} * d(S^i, C^j)$$

Where, μ_{ij} specifies the membership function of i^{th} data point in the j^{th} cluster and $d(S^i, C^j)$ denotes the JS between the data points S^i and the cluster centroids C^j.

Step 4: The JS is estimated as follows,

$$d(S^i, C^j) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} S^i * C^j}{\sqrt{\sum_{i=1}^{N} \left\| S^i \right\|^2} * \sqrt{\sum_{j=1}^{M} \left\| C^j \right\|^2} - \sum_{i=1}^{N} \sum_{j=1}^{M} S^i * C^j}$$

Step 5: The membership function μ_{ij} is evaluated using the below equation,

$$\mu_{ij} = \sum_{k=1}^{n} \left(\frac{d(S^i, C^j)}{d(S^i, C^k)} \right)^{-\frac{2}{f-1}}$$

Where f shows the fuzziness index, C^k exemplifies the k^{th} cluster center.

5.2.3 Cluster Head Selection

Following the clustering of SNs, the Boosted Grasshopper Optimization (BGOA) technique is used to select CHs. The CHs gather data from the cluster's nodes and transmit it to the BS. Grasshopper optimization (GOA) is a meta-heuristic optimization algorithm inspired by grasshoppers' food-finding behaviour. The grasshopper takes small steps and moves slowly in its larval stage. Grasshoppers move locally in the exploitation stage, while they move quickly towards the food source in the exploration stage. Here the GOA uses a logistic map to improve the exploitation abilities of the approach by identifying the optimal solution. Moreover, GOA introduces an inertial weight to enhance the proper balance between the exploration and exploitation stages. The flow chart of the proposed BGOA is given in Figure 4.

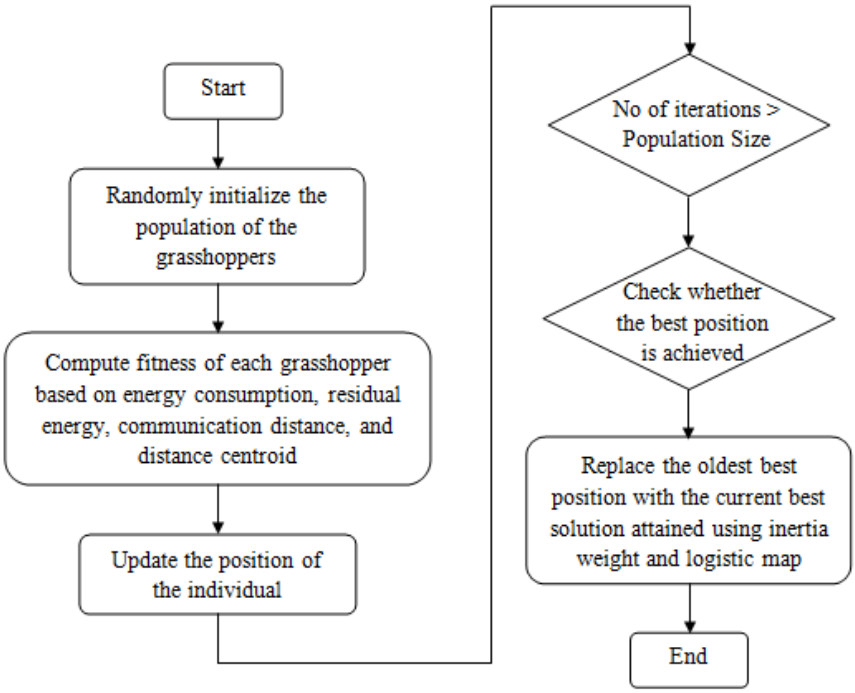

Start
Randomly initialize the population of the grasshoppers
Compute fitness of each grasshopper based on energy consumption, residual energy, communication distance, and distance centroid
Update the position of the individual
No of iterations > Population Size
Check whether the best position is achieved
Replace the oldest best position with the current best solution attained using inertia weight and logistic map
End

Figure 4: Flowchart of the proposed BGOA

5.2.4 Node Authentication

When the SNs begin transmitting messages, the BS performs node authentication. During this phase, the SNs send a message transmission request to the BS via selected CHs. The BS authenticates the SN at this point by using the secret key generated during registration. If the secret key matches the SN's ID, the BS accepts the request for DT from the SN. The BS rejects the request and sends the alert to the CH node if the SN's secret does not

match. The CH then uses the unique identity number of SNs to identify the malicious node and ignores communication with it.

5.2.5 Data Encryption using SHECC

Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic technique based on elliptic curves' algebraic structure. Each node has its own set of public and private keys, which are used in the encryption and decryption processes. Because of its faster and smaller key generation, ECC is considered for data security in the proposed model. After successful authentication, the Secure Hashing Elliptic Curve Cryptography (SHECC) method encrypts the data for secure transmission in the network. The security hashing (SH) function is multiplied during encryption and divided during decryption to add more security to the traditional ECC technique. The model SHECC refers to the variation made (SH) in the baseline ECC.

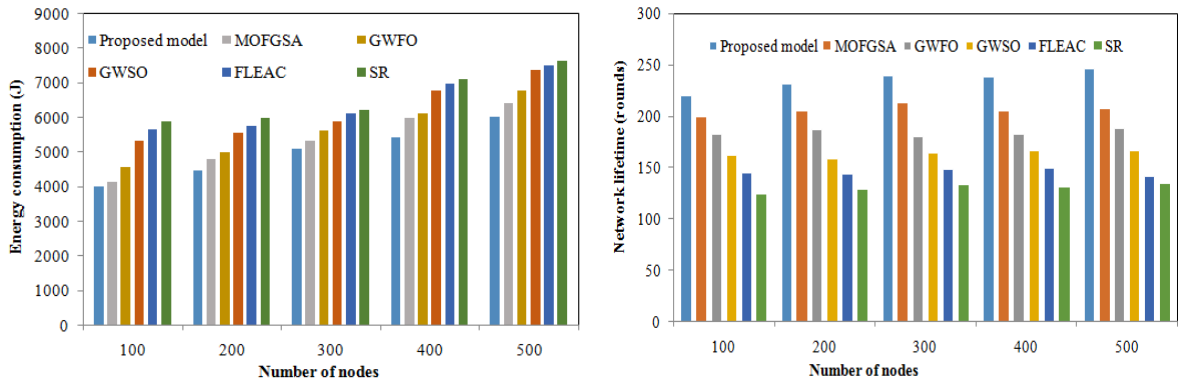
5.2.6 Blockchain-Enabled Secure Cloud Storage

The proposed model uses the BC in the cloud for storing the authentication credentials entered at the time of registration and the encrypted data received from the BS. In an open data network, BC is defined as a distributed ledger that includes several consecutively connected blocks to provide secure computing with no centralized authority. A block is made up of two parts: a block header and a block body. Block version, timestamp, Merkle tree (MT) root hash, bits, nonce, and parent block hash are all included in the block header. The BC network then generates a unique hash using the SHA256 algorithm. Then, all hash values are linked through an initial hash value, resulting in an unbreakable network of transactions. Once a transaction record is added to a block, the block is successfully generated and committed to the BC. This procedure creates a decentralized system that is both secure and dependable.

5.2. Performance Evaluation

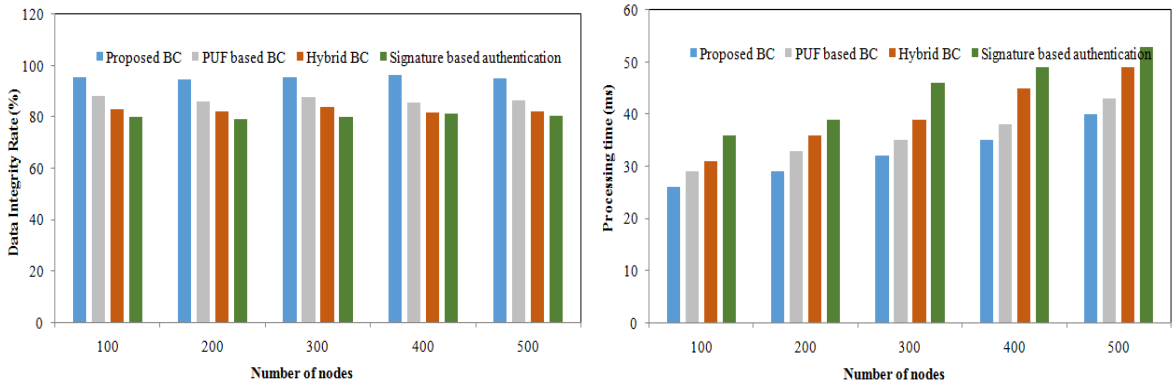
The proposed work is implemented in the Network Simulator-3.26 (NS-3.26), the event-based simulation tool that supports a variety of network simulations. The SNs and IoT devices were dispersed inside the IoT-linked WSN network with a size of 100×100 m^2. The BS is located at the center of the network. In total, 500 SNs are considered, and the transmission range of each SN is set to 200m. The implementation results (Figure 5a and Figure 5b) of the proposed model are compared with the existing models to prove the EE and

QoS performance of the proposed system. The existing approaches used for comparison are FLEAC [10], MOFGSA [11], GWFO [12], GWSO [13], and secure routing [14].



(a) (b)

Figure 5: Energy consumption and network lifetime of the techniques



(a) (b)

Figure 6: Data integrity rate and processing time of the BC-based authentication schemes

The work also analyses the performance of the proposed BC-based data storage system (Figure 6a and Figure 6b) by comparing the model with the existing BC model. The models used for comparison are PUF-based BC [15], Hybrid BC [16], and signature-based BC [17], and the metrics used for comparison are data integrity rate and processing time. From the results, it is concluded that the presented model achieves better QoS, higher security and lower EC by overcoming the challenges and problems faced by the existing models.

5.3 An Efficient Blockchain-based BSLA System in WSN with LTK-RNN based Attack Detection and CMAES based Security Models

Here an efficient and secure BC-based Binary Shift Left Authentication (BSLA) protocol along with Logistic TanH Kaiming initialized Recurrent Neural Network (LTK-RNN) for attack detection in IoT-assisted WSNs is proposed. In addition, Chebyshev Mapping-induced Advanced Encryption Standard (CMAES) is proposed for providing data security. At first, all the SNs that are deployed in the WSNs have registered their details with the nearest BS. The registration details of the SNs are further stored in the BC network for security. Afterwards, during DT time, the SNs authentication is carried out in the BC utilizing the BSLA technique. After successful authentication, the sensed data undergoes an attack detection system, in which feature extraction, feature selection, and classification are made to identify attacked and non-attacked data. Then, the attacked data is stored in the log file, and the non-attacked data undergoes the CMAES encryption technique for secure storage in the cloud server. The architecture of the proposed model is given in Figure 7.

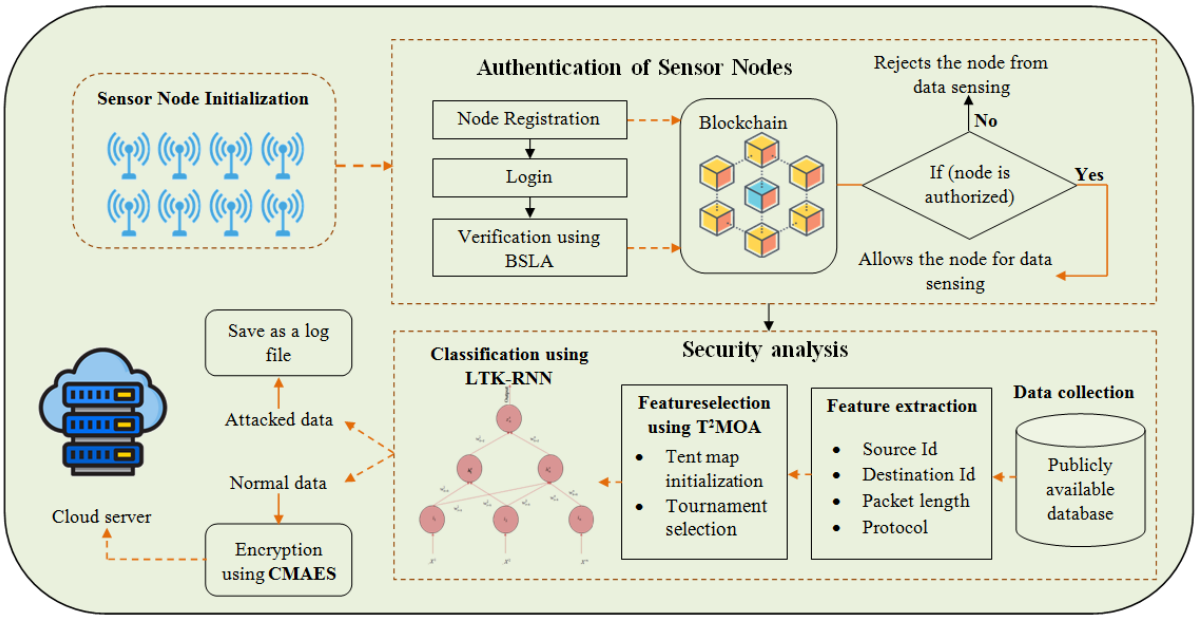


Figure 7: Architecture of the proposed LTK-RNN attack detection system with BC based authentication

5.3.1 Registration

For the registration of SNs, at first, the BS generates its own private and public keys represented as $\tau_r(b)$, $\tau_{pub}(b)$ respectively. Then, the BS calculates the secret system

parameter (α) by multiplying and squaring its own private and public keys. After that, the BS registers all the valid SNs by generating the public and private keys for each node. The public and private keys of all the SNs are mathematically notated as $\kappa_n(i), \delta_{nr}(i)$ in that order. Next to key generation, a secret key (γ) is generated by using the following equation,

$$\gamma = \left\{ \left(\delta_{nr}(i) * \alpha \right)^{\kappa_n(i)} + \eta_i \right\}$$

Then, this secret key is transformed into binary form, and the shift left operation is carried out. In shift left operation, the first operand of the specified number of bits is shifted to the left, and the excess bits shifted off to the left are removed. Finally, each node's shifted binary form of secret keys is stored in the BC server. And then, this secret key (γ) is securely forwarded to the corresponding nodes.

5.3.2 Login Phase

Once all the SNs are registered with the BS, login is carried out for efficient DT between each node and BS. At the time of login, the node generates a login request along with the time stamp (t) to the BS. The timestamp is the time the request is sent, which ensures avoiding the reply attack. Upon sending the request, the BS first checks its registration list to make sure that the node is already registered. The login request consists of node ID (η_i) and password (p_i). If the node is already registered with the BS, then the node login becomes successful. If the node registration is not successful, then the request is declined by the BS, and the incoming request is considered an attack and removes the node from the network. Once login is done, authentication of the SN takes place by the BS.

5.3.3 BSLA based Verification

- To authenticate SN (φ_i), at first, the BS requests the secret key (γ) of the corresponding SN along with its registration details and time stamp (t). BS first checks the registration list to make sure that the φ_i sent details are already registered.
- The SN registration, login, and authentication processes take place in the BC sever, which is detailed further. If the node is registered, it checks whether the secret key matches that particular node's registered secret key. If both the secret keys are the same, then authentication becomes successful, and DT is carried out.

5.3.4 Blockchain

- BC technology offers practical solutions for identity authentication and security protection in WSNs. Each time a new device is included in the network, its identity information must be registered with the BC. The BC ledger stores every device's ID, private key, public key, base station's ID, binary shifted secret key and other information. A binary shifted secret key can be used for identity authentication between nodes every time peer-to-peer communication happens. If a device wants to connect with a network, then it will be authenticated with the help of the registration information of BC.

- After the authentication process, a device's integrity will be verified to detect intrusion behaviour. The private keys are encrypted and locally kept, while the public key is kept in the BC ledger. When BS receives the authentication request from the SNs, the public key φ_i is searched first in the local BC ledger by a BS according to the ID of φ_i . If the public key is obtained, BS will verify the identity, and then secret key verification is carried out. Figure 8 illustrates the general architecture of BC-based cloud data storage.

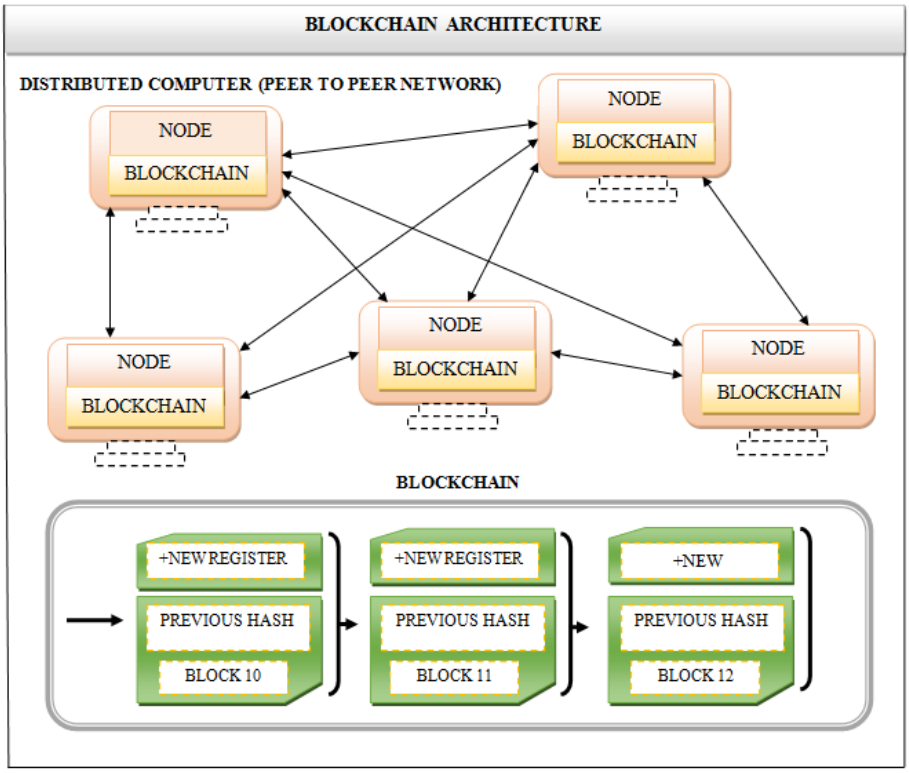


Figure 8: Blockchain architecture

5.3.5 Security Analysis Phase

After SN authentication, the sensed data is checked for security. That is, whether the data gets attacked during transmission is checked in this phase. This can be done using the trained security analysis system in the cloud server. In the training phase of the proposed security analysis system, data collection, feature extraction, feature selection, as well as classification are performed. The dataset required to train the proposed security analysis system is primarily collected from publically available sources. While testing, the data from the SN is used. Next, features are extracted from the input dataset for processing. Feature extraction is the procedure of detecting the data characteristic required to classify the type of data. The features, such as source ID, destination ID, packet length, protocol, etc., are extracted from the dataset.

5.3.6 Feature Selection by T^2MOA

After feature extraction, the most relevant features are selected using the T^2MOA technique, which improves the detection accuracy and reduces the time required to process the data. On the other hand, the random initialization of the mayfly population may result in population diversity and slow down the algorithm's convergence speed. Furthermore, during the mating stage of mayflies, incorrect pair selection may reduce the technique's exploration and exploitation ability. Therefore, to initialize the population, a Tent map was used in the proposed model that evenly distributed the agents and extended the mayflies' search range. Then, a tournament selection approach was included for screening the superior solution in the mating stage of mayflies, which balances the global search process and local development capabilities well. Due to these modifications made in the conventional MOA, the proposed algorithm is named T^2MOA. The pseudocode of the proposed model is given below.

Pseudocode of proposed T^{2}MOA

Input: Extracted features $\left(x^i\right)$

Output: Optimized features $\left(X^k\right)$

Begin
Generate initial mayfly population
Compute $f(\lambda)=\lambda * \min\left(x^i,\ 1-x_i\right)$
Initialize position vector $\left(x'^{ik}\right)$ and velocity $\left(v_t^{ik}\right)$
Calculate the fitness of each mayfly
Recognize $x'^{ik}(lbest)$ and $x'^{ik}(gbest)$
While $t < t_{\max}$
    For each i
        Update $v_t^{ik} \rightarrow v_{t+1}^{ik}$
        Execute $x'^{ik}_{t+1} = x'^{ik}_t + v^{ik}_{t+1}$
        Perform nuptial movement
        Modernize $y_t^{ik} \rightarrow y_{t+1}^{ik}$
        Estimate $p_i(t)=\dfrac{Z_t^{ik}}{\sum_i Z_t^{ik}}$ for mutation
        Produce ϕ^1, ϕ^2
        Replace the worst solution with optimal solution
        Renew $x'^{ik}(lbest)$ and $x'^{ik}(gbest)$
    End for
End while
Attain $X^k = X^1, X^2, \ldots\ldots, X^m$
End

5.3.7 Classification by LTK-RNN

A recurrent Neural Network (RNN) is influenced by the weights applied to the input, the hidden states, and the bias representing the input or output. Therefore, the bias and weight values are randomly initialized, leading to slower computation. Moreover, the activation function used in the general RNN is a parametric function, which congregates with the sign function as the parameter goes to infinity. The proposed work initializes the weight values by employing the Kaiming-initialization technique to overcome the downside in the conventional RNN. Also, Logistic Tanh (LT) activation function is adapted instead of the parametric function. Hence, the resultant modified technique is renamed LTK-RNN. The

algorithmic process of LTK-RNN is explained as follows.

Step 1: The optimized features $\left(X^k\right)$ are given as input to the LTK-RNN network, where it estimates the hidden vector sequence $\left(h^t\right)$ and the output vector sequence $\left(z^t\right)$ at a time $t = 1,2,\ldots\ldots,T$ by using the following equations,

$$h^t = \delta\left(w_{i-h}x^k + w_{h-h}h^{t-1} + b_h\right)$$

$$z^t = w_{h-z}h^t + b_z$$

Where, $\delta(\bullet)$ indicates the LTH activation function, w represents the weight indices that are initialized using the He-initialization technique, w_{i-h} is the input-hidden weights, w_{h-h} mentions the weight in the hidden layer, w_{h-z} shows the hidden-output weights, b_h, b_z is the hidden and output layer bias functions respectively, and h^{t-1} depicts the previous state $(t-1)$ hidden layer function.

Step 2: The LT activation function is formulated using below equation,

$$\delta\left(h^t\right) = \frac{1}{1+\exp\left(-2h^t\right)}$$

Step 3: The Kaiming-initialization technique is expressed as,

$$\mathrm{var}(w) = \left(\frac{2}{N_t}\right)^{0.5}$$

Where, $\mathrm{var}(w)$ determines the variance of weights and N_t is the number of neurons in the network.

5.3.8 Data Encryption through CMAES

The encryption of normal data is performed here using CMAES. The AES algorithm has been chosen as a standard among other symmetric cipher algorithms due to its high performance. The traditional AES algorithm generates fixed keys for encryption that the sender and receiver share. As a result, the key is easily stolen. The proposed work creates the encryption key using a Chebyshev mapping sequence to enhance the security level of the key. This modification not only diminishes the algorithm's time complexity but also includes diffusion capability to the presented model, making the encrypted data resistant to differential

attacks.

5.3.9 Performance Evaluation

The performance investigation is made utilizing performance metrics such as accuracy, f-measure, and Root Mean Square Error (RMSE). The outcomes obtained by the proposed LTK-RNN technique for security scrutiny are compared with existing attack detections models such as GRU, DRBN, and OLWPR. The comparison of accuracy (Ac) and f-measure (F_m) are graphically represented in Table 1. The analysis demonstrates that the scheme is resistant to several well-known attacks and achieves a maximum accuracy of 96.457%.

Table 1: Performance study based on accuracy and f-measure

Number of nodes/ Techniques	**Proposed LTK-RNN**		**GRU**		**DRBN**		**OLWPR**	
	Ac (%)	F_m (%)	Ac (%)	F_m (%)	Ac (%)	F_m (%)	Ac (%)	F_m (%)
100	96.324	95.897	88.635	87.325	90.857	89.654	94.657	93.857
200	96.124	95.236	88.745	86.574	89.587	90.324	94.237	93.254
300	95.632	96.234	88.914	86.547	90.857	89.745	93.748	94.234
400	96.457	95.784	87.544	87.124	90.471	89.657	93.454	93.897
500	95.244	96.324	87.958	87.324	89.745	90.322	93.457	93.157

ORGANIZATION OF THESIS

Chapter 1: *"Introduction"* presents the concepts of WSNs and IoT, challenges, security issues, problems of existing models, and necessity of BC mechanism and QoS parameters.

Chapter 2: *"Literature Review"* presents the various research perspective of various researchers put forwarded on clustering, CH selection, authentication and data security.

Chapter 3: *"Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm*" describes the framework for providing data

security in IoT using an integration of SDN based BC mechanism and ECIES and thereby evaluate under various performance measures with other existing methods.

Chapter 4: "*QoS aware secure data transmission model for IoT assisted wireless sensor networks*" describes the framework for providing QoS aware secure data security mechanism for IoT assisted WSNs using an effective BGOA based clustering approach and BC based SHAECC data security model. The performance evaluations are made under various performance measures with other existing methods. Also, we briefly describe the concluded version and the future scope of the propose framework.

Chapter 5: "An efficient blockchain-based BSLA system in WSN with LTK-RNN based attack detection and CMAES based security models

" describes the framework of BC based BSLA protocol for data security with an inclusion deep learning model based attack detection scheme for WSNs. The performance evaluations are made under various performance measures with other existing methods. Also, we briefly describe the concluded version and the future scope of the propose framework.

Chapter 6: "*Conclusions and Future Scope*" presents the overall conclusion of the thesis and the future scope of proposed frameworks for much larger scale implementation

REFERENCES

1. Ding Wang, Ping Wang and Chenyu Wang, Efficient Multi-Factor User Authentication Protocol with Forward Secrecy for Real-Time Data Access in WSNs, *ACM Transactions on Cyber-Physical Systems*, **4** (3) (2020), 1-26.

2. RuhulAmin and Biswas G. P, A Secure Light Weight Scheme for User Authentication and Key Agreement in Multi-Gateway based Wireless Sensor Networks, *Ad Hoc Networks*, **36** (2015), 58-80, doi.org/10.1016/j.adhoc.2015.05.020.

3. Irin Loretta G and Kavitha V., Privacy Preserving using Multi-Hop Dynamic Clustering Routing Protocol and Elliptic Curve Cryptosystem for WSN in IoT environment, *Peer to Peer Networking and Applications*, **14** (2) (2021), 821-836.

4. Mukaram Safaldin, Mohammed Otair, and Laith Abualigah, "Improved Binary Gray Wolf Optimizer and SVM for Intrusion Detection System in Wireless Sensor Networks, *Journal of Ambient Intelligence and Humanized Computing*, **12** (2) (2020), 1559-1576.

5. Baybars Karabekir, Muhammed Ali Aydın, and Abdül Halim Zaim, Energy-Efficient Clustering-based Mobile Routing Algorithm for Wireless Sensor Networks, *Electrica*, **21**(1) (2021), 41-49.

6. Lakshmi M and Prashanth C R, Energy-Efficient Clustering-Based Mobile Routing Algorithm for Wireless Sensor Networks, *International Journal of Computer Networks & Communications*, **13** (1) (2021), DOI: 10.5121/ijcnc.2021.13105.

7. Liangqin Gong, Daniyal M. Alghazzawi, and Li Cheng, BCoT Sentry: A Blockchain-based Identity Authentication Framework for IoT Devices, *Information*, **12** (5) (2021), 203.

8. Libo Feng, Hui Zhang, Liqi Lou, and Yong Chen, A Blockchain-based Collocation Storage Architecture for Data Security Process Platform of WSN, *IEEE 22nd International Conference on Computer Supported Cooperative Work in Design* ((*CSCWD*)), (2018), 75-80.

9. I. D Buldin, M. G. Gorodnichev, S. S. Makhrov, and E. N. Denisova, "Next Generation Industrial Blockchain-based Wireless Sensor Networks," *Wave*

Electronics and Its Application in Information and Telecommunication Systems (WECONF), (2018), 1-5.

10. Bharat Bhushan, and Gadadhar Sahoo. FLEAC: Fuzzy Logic-based Energy Adequate Clustering Protocol for Wireless Sensor Networks using Improved Grasshopper Optimization Algorithm, *Wireless Personal Commun*ications, (2021), 1-34.
11. Amol Dhumane V and Rajesh S. Prasad, Multi-Objective Fractional Gravitational Search Algorithm for Energy Efficient Routing in IoT, *Wireless Networks*, **25** (1) (2019), 399-413.
12. Kavita Jaiswal, and Veena Anand, A Grey-Wolf based Optimized Clustering Approach to Improve QoS in Wireless Sensor Networks for IoT Applications, *Peer to Peer Networking and Applications*, **14** (4) (2021), 1943-1962.
13. Mohana Bakshi, Chandreyee Chowdhury, and Ujjwal Maulik, Energy-Efficient Cluster Head Selection Algorithm for IoT using Modified Glow-Worm Swarm Optimization', *The Journal of Supercomputing*, **77** (7) (2021), 6457-6475.
14. Vasim Babu M, Jafar A. Alzubi, Ramesh Sekaran, Rizwan Patan, Manikandan Ramachandran, and Deepak Gupta, An improved IDAF-FIT Clustering based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network, *Mobile Networks and Applications*, **26** (3) (2021), 1059-1067.
15. Akash Suresh Patil, Rafik Hamza, Alzubair Hassan, Nan Jiang, Hongyang Yan, and Jin Li, Efficient Privacy-Preserving Authentication Protocol using PUFs with Blockchain Smart Contracts, *Computers & Security*, **97** (2020),101958.
16. Azath Mubarakali, An Efficient Authentication Scheme using Blockchain Technology for Wireless Sensor Networks, *Wireless Personal Communications*, (2021), 1-15, doi.org/10.1007/s11277-021-08212-w.
17. Qing Fan, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo, A Secure and Efficient Authentication and Data Sharing Scheme for Internet of Things based on Blockchain, *Journal of Systems Architecture*, **117** (2021), 102112, doi.org/10.1016/j.sysarc.2021.102112.

18. Semih Cakir, Sinan Toklu, and Nesibe Yalcin, RPL Attack Detection and Prevention in the Internet of Things Networks using a GRU based deep learning, *IEEE Access*, **8** (2020), 183678-183689.

19. Premkumar M. and T. V. P. Sundararajan, Defense Countermeasures for DoS Attacks in WSNs using Deep Radial Basis Networks, *Wireless Personal Communications*, **120** (4) (2021), 2545-2560.

20. I. Gethzi Ahila Poornima, and B. Paramasivan, Anomaly Detection in Wireless Sensor Network using Machine Learning Algorithm, *Computer Communications*, **151** (2020), pp. 331-337.

LIST OF PUBLICATIONS

1. Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. (2022,September). “Quality of Service aware secure data transmission model for Internet of Things assisted wireless sensor networks” . Transactions on Emerging Telecommunications Technologies (ETT) – Wiley (SCIE : 3.310).
2. Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. (2020, August). “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm”. Materials Today: Proceedings – Elsevier (Scopus).
3. Velmurugadass P, Dhanasekaran S, D. Gnanasekaran. (2022,March). “Edge Computing With Cloud Based Machine Learning With IOT Infrastructure Security Issue”. Sustainable Development in Engineering And Technology -3Ciencias (WoS).
4. Velmurugadass P, Dhanasekaran S. (2021, October). “Enhancing Security Service of Data Protection Level using Machine Learning” 2021 2nd Global Conference for Advancement in Technology, GCAT. IEEE (Scopus).
5. Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. (2022, June). “An Efficient Blockchain-based BSLA System in WSN with LTK-RNN Based Attack Detection and CMAES based Security Model “. International Journal of Computer Network and Information Security – MECS (Scopus).